REMARKS/ARGUMENTS:

The following referenced telephone interview took place on September 14, 2006.

Substance of the Telephone Interview

The undersigned attorney and the Examiner discussed claims 1, 35, 43, and it was agreed to amend same to remove "trusted" from claim 1, line 8, and to revise the first occurrence of "said service provider" in claims 35 and 43 to read "a service provider".

The undersigned attorney and the Examiner also discussed claims 31 and 41, and it was decided to amend both in a similar manner to refer to charging and reporting, in a manner somewhat similar to the language found in, for example, claim 35. Claims 31 and 41 are also amended above.

The foregoing amendments are herewith made to ensure that the amendments are entered. If the Examiner has already made these amendments by Examiner's Amendment, then the foregoing amendments may be ignored.

In the Office Action dated October 20, 2006, the Examiner has rejected the pending claims 1-16 and 18-44. More specifically, the Examiner rejected claims 1-9, 16, 19-24, 31-38 and 41-44 under 35 USC 103(a) as being unpatentable over Tamaki (US2003/0054796) in view of Dahan (US2004/0123118); claims 10-11, 25-26, and 39-40 under 35 USC 103(a) over Tamaki in view of Dahan and in further view of Kirkup (US20040142686); claims 12-13 and 27-28 under 35 USC 103(a) over Tamaki in view of Dahan and in further view of Sakakura (JP2002209028); claims 14 and 29 under 35 USC 103(a) over Tamaki in view of Dahan, Sakakura and in further view of Piazza (US2003/0061358); and claims 15, 30 are rejected under 35 USC 103(a) as being unpatentable over Tamaki in view of Dahan, Sakakura and in further view of Von Kaenel (US20040117358). Respectfully, we traverse the rejection.

In the rejection of the claims including the independent claims 1, 16, 31, 35, 41 and 43 the Examiner acknowledges that Tamaki et al. does not teach the use of trusted software, but then states that this limitation is taught by Dahan in paragraph [0011]. The Examiner then further states that it would have been obvious to apply the teachings of Dahan to Tamaki in order to "to improve security for the network".

In the paragraph cited by the Examiner, Dahan discloses:

> **A secure execution mode is thus provided on a platform where the only trusted software is the code stored in on-chip ROM. An indicator means observable by a user of the digital system is provided, wherein the indicator means can only be activated by the trusted program code while in the secure mode of operation.**

Dahan discloses a security limitation of the prior art as "On a smart device enabled for a secure class of applications such as for m-commerce (mobile commerce) or e-banking (electronic banking), the user is asked to enter secret information such as a password on the keyboard or to sign messages displayed on the screen. When doing so, the user has no other choice then to fully rely on the integrity of his device. However, there is no way for the user to detect that a hacker or a virus has defeated the security framework of his device" (par. [0009]). Dahan discloses "Thus, improvements in system security are needed" (par. [0010]), and further discloses:

> **"In general, and in a form of the present invention, a digital system is provided with a secure mode (3rd level of privilege) built in a non-invasive way on a processor system" (par. [0011]).**

Dahan discloses that "In secure mode, the access to a physical user interface such as a keyboard or display are restricted to secure applications through trusted drivers ... Otherwise, if a virus/hacker manages to download a forged driver on the smart device, then the user has no way to know that he cannot rely on his device" (par. [0022]). In addition, the "ROM is partitioned in two parts: a secure portion of the ROM that is protected by the secure bit and can only be accessed in secure mode; and a public portion of the ROM that is always accessible and contains the boot area" (par. [0054])" Therefore, "The secure mode is entered when security signal 302 is asserted" and "In secure mode, CPU 200 can only execute code that is stored in secure ROM 310 or secure SRAM 312" (par. [0053]).

A method is disclosed in Dahan "for protecting sensitive information from access by non-trusted software" and to provide that "There can exist no possible flows by which non-trusted code can either fool the hardware into entering secure Mode, or get trusted code to perform tasks it shouldn't." (paragraphs [0044] and [0045]). Dahan thus discloses a technique to restrict access to, and prevent tampering with a digital device.

In the office action, the Examiner acknowledges that Tamaki does not teach the use of trusted software. However, it has been shown that Dahan uses a hardware implementation to secure a digital device (paragraphs [0022] and [0044]). Therefore, even if the "secure execution mode" of Dahan were incorporated into at least one of the end user terminals 111-114 and into the personal communications providers terminals 115-117 of Tamaki et al., which is not admitted is suggested, the resulting modified terminals would appear to simply facilitate a secure mode on the terminal itself (Dahan paragraphs [0044] and [0045]). Clearly, there is no suggestion in such a proposed modification that there would be executed, as claim 1 recites in part:

> **"<u>establishing a trusted service provisioning relationship between the user device and a bridging user device through a first wireless network;</u>**
> **providing a desired service for the user device with the service provider via the bridging user device and the first wireless network, and through a second wireless network that couples the bridging user device to the service provider;**

> **while providing the service, recording charging data for the service provisioning relationship between the user device and the bridging user device; and**
>
> **reporting the charging data from the bridging user device to the service provider, where at least establishing and recording use trusted software comprising a certified unit of code running on the user device and on the bridging user device."**

Thus, for the reasons stated Tamaki in view of Dahan does not disclose or suggest claim 1. That is, at least for the reason that if the proposed combination of Tamaki and Dahan were made, at most the terminals of Tamaki would be operational, in a "secure mode," so that "access to a physical user interface such as a keyboard or display are restricted to secure applications through trusted drivers" (Dahan at paragraph [0022]). Without expressly or impliedly admitting that the proposed combination is suggested, clearly the proposed combination would not render obvious at least the subject matter that is highlighted above for claim 1.

In addition, for at least the reasons stated above Tamaki in view of Dahan does not disclose or suggest, as claim 16 recites in part:

> **"where said user device, said bridging user device and said service provider execute computer code to establish a trusted service provisioning relationship between said user device and to record charging data for the trusted service provisioning relationship between said user device and said bridging user device; and to report the charging data from said bridging user device to said service provider, where said computer code comprises trusted software comprising a certified unit of code running on said user device and on said bridging user device"**

In addition, for at least the reasons stated above Tamaki in view of Dahan does not disclose or suggest, as claim 31 recites in part:

> **said memory storing computer code executable by said data processor to request a service to be provided by a service provider and to establish a service provisioning relationship between said mobile device and another device through said short range wireless network, where said another device is bidirectionally coupled to said service provider through a second wireless network, and where said service is provided for said mobile device by the service provider via said short range wireless network, said another device, and said second wireless network, where said computer code comprises trusted software comprising a certified unit of code running on said mobile device and on said another device, and where said another device is operable to record charging data related to the service provisioning relationship between said mobile device and said another device, and to report the charging data to said service provider.**

In addition, for at least the reasons stated above Tamaki in view of Dahan does not disclose or suggest, as claim 35 recites in part:

> **said memory storing computer code executable by said data processor to establish a service provisioning relationship between said mobile device and another device through said short range wireless network, said computer code comprising trusted software comprising a certified unit of code running on said mobile device and on said another device, where said mobile device can be bidirectionally coupled to a service provider through said cellular wireless network, and where said service is provided for said another device by the service provider via said short range wireless network, said mobile device and said cellular wireless network, and where said computer code executable by said data processor further is operable to record charging data for the**

> **service provisioning relationship between said mobile device and said another device, and to report the charging data to said service provider via said cellular wireless network.**

In addition, for at least the reasons stated above Tamaki in view of Dahan does not disclose or suggest, as claim 41 recites in part:

> **a service to be provided by a service provider and to establish a service provisioning relationship between said mobile terminal and a device through said short range wireless network, where said device is bidirectionally coupled to said service provider through another wireless network, and where said service is provided for said mobile terminal by the service provider via said short range wireless network, said device and said another wireless network, where said data processor operates under control of trusted software comprising a certified unit of code stored in said mobile terminal and in said device, and where said device is operable to record charging data related to the service provisioning relationship between said mobile terminal and said device, and to report the charging data to said service provider.**

In addition, for at least the reasons stated above Tamaki in view of Dahan does not disclose, as claim 43 recites:

> **A mobile terminal comprising a data processor coupled to an interface to a short range wireless network and to an interface to a cellular wireless network, said data processor operable to establish a service provisioning relationship between said mobile terminal and a device through said short range wireless network, where said mobile terminal can be bidirectionally coupled to a service provider through said cellular wireless network, and where said service is provided for said device by the service provider via said**

> **short range wireless network, said mobile terminal and said cellular wireless network, <u>and where said data processor is further operable to record charging data for the service provisioning relationship between said mobile terminal and said device, and to report the charging data to said service provider over said cellular wireless network, where said data processor operates under control of trusted software comprising a certified unit of code stored in said mobile terminal and in said device.</u>**

Tamaki in view of Dahan does not disclose or suggest the subject matter found in claims 1, 16, 31, 35, 41 and 43; and all the claims 1, 16, 31, 35, 41 and 43 should be allowed.

It is further noted that in the rejection of claim 21 the Examiner states that Tamaki teaches the method as in claim 1 citing "figures 3 & 5 and paragraphs [0031]-[0033], [0035]." Respectfully the applicant disagrees with the Examiner.

Claim 21 recites:

> **"A system as in claim 16, where said computer code that establishes said service provisioning relationship includes computer code for negotiating specifics of charging for said service provisioning relationship between said user device and said bridging user device using an offer-counteroffer technique."**

In the reference cited by the Examiner, Tamaki discloses "The end users and personal communications service providers pay three types of fees according to the bill from the communications service provider: a utilization fee for communications service provider, a utilization fee for information service provider and a utilization fee for personal communications service provider" (par. [0033]). In addition, Tamaki discloses that "In order to receive low-priced communications service offered by the ad hoc network of terminals with repeater function owned by personal communications service providers, the end users and personal communications service providers take the registration procedure for personal communications service provider and make a contract to pay a monthly fee based on the flat rate system to the communications service provider" (par. [0035]). Thus, Tamaki does not disclose **"negotiating specifics of charging for said service provisioning relationship between said user device and said bridging user device using an offer-counteroffer technique."** as claim 21 recites in part.

Tamaki merely discloses that the users can agree to contract on a monthly basis to receive a discount (par. [0035]). Clearly, Tamaki does not disclose or suggest any negotiation of the charging specifics as in claim 21, in particular a negotiation between a user device and a bridging user device.

The Examiner rejects claims 14 and 29 under 35 USC 103(a) over Tamaki in view of Dahan, Sakakura and in further view of Piazza. Respectfully the applicant disagrees.

The Piazza reference cited by the Examiner states: "To prevent the transmission of clear text passwords and to secure information, all transactions including the initial password exchange are encrypted with, for example, SSL (Secure Sockets Layer) 3.0. 128-bit encryption" (par. [0150]). However, the Examiner has failed to consider whether Dahan would function when "all transactions including the initial password exchange are encrypted with, for example, SSL (Secure Sockets Layer) 3.0. 128-bit encryption" as Piazza discloses.

Dahan discloses "The security state machine monitors various signals 330 from processor 200's external interfaces and in particular, the addresses fetched by the processor on the instruction bus" (par. [0052]). Further, "The security state machine is tightly coupled to low-level assembly code from the entry sequence" and "It reacts to events generated by the entry sequence on the monitored signals" (par. [0052]). There is no disclosure in Dahan to indicate that the Security State Machine would be able to process "all transactions including the initial password exchange ... encrypted with, for example, SSL (Secure Sockets Layer) 3.0. 128-bit encryption" as Piazza discloses. As Dahan discloses a method "for protecting sensitive information from access by non-trusted software," it would appear to be counter to this method to allow an unreadable encrypted data stream to access the secured device in Dahan. Dahan does not disclose or suggest that "all transactions including the initial password exchange" encrypted using SSL 128-bit encryption would be allowed access to the digital device in Dahan. As claims 14 and 29 recite this feature; the reference Tamaki in view of Dahan, Sakakura and in further view of Piazza does not disclose, teach or suggest claims 14 and 29; and claims 14 and 29 should be allowed.

The applicant provides notice that the indicated allowability of the claims for these reasons alone should not be construed as an acknowledgment that the Applicant is in agreement with the Examiner's other reasons for rejecting the claims based variously on Tamaki and the other cited documents.

For the reasons stated above, and for the reason that the claims 2-15, 18-30, 32-34, 36-40, 42 and 44 depend from claims 1, 16, 31, 35, 41 and 43 respectively; all the claims 1-16 and 18-44 should be allowed.

Respectfully submitted:

Harry Smith

Harry F. Smith
Reg. No.: 32,493

12/13/2006
Date

Customer No.: 29683
HARRINGTON & SMITH, LLP
4 Research Drive
Shelton, CT 06484-6212
Phone: (203) 925-9400
Facsimile: (203) 944-0245 Email: hsmith@hspatent.com

S.N. 10/792,181
Art Unit 2617

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

12/13/2006
Date

Elaine Y. Mian
Name of Person Making Deposit